

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claim 1 (currently amended) A method for processing network packets on a computer network, comprising:

transferring the network packets over ~~the computer network~~ a virtual private network (VPN) based on a policy wherein network packets having a high priority are transferred before network packets having a low priority; and

performing cryptographic processing of the network packets using the policy;

determining whether newly arrived network packets have a higher priority than a current network packet being processed; and

suspending processing of the current network packet and beginning processing of the newly arrived network packets in response to one or more newly arrived network packets having a higher priority than the current network packet.

Claim 2 (original) The method of claim 1, wherein cryptographic processing includes encryption and decryption of network packets.

Claim 3 (original) The method of claim 1, wherein cryptographic processing is performed such that processing of the network packets having a low priority are suspended in favor of the network packets having the high priority.

Claim 4 (original) The method of claim 1, wherein the policy is a quality of service policy model.

Claim 5 (canceled).

Claim 6 (original) The method of claim 5, further comprising determining that a higher-priority packet than the network packet being processed is available to have cryptographic processing performed and suspending processing of the network packet being processed and processing instead the higher-priority network packet.

Claims 7-11. (canceled).

Claim 12 (currently amended) A network packet management system for managing network packets on a computer network, comprising:

a quality of service policy module that contains priority policies for handling of the network packets;

a quality of service module in communication with the quality of service policy module that manages the sequencing of the network packets over a virtual private network (VPN) of the computer network based on the priority policies; and

a internet Internet protocol security module in communication with the quality of service policy module that manages the encryption and decryption of the network packets based on the priority policies that includes determining whether newly arrived network packets have a higher priority than a current network packet being processed, suspending processing of the current network packet and beginning processing of the newly arrived network packets in response to one or more newly arrived network packets having a higher priority than the current network packet.

Claim 13 (currently amended) The network packet management system of claim 12, wherein the internet Internet protocol security module comprises an encryption module for encrypting network packets and a decryption module for decrypting network packets.

Claim 14 (original) The network packet management system of claim 12, wherein the priority policies are based on a quality of service policy model.

Claim 15 (currently amended) The network packet management system of claim 12, wherein the priority policies are regulations that govern the order in which network packets are processed by the quality of service module and the ~~internet~~ Internet protocol security module.

Claim 16 (original) The network packet management system of claim 15, wherein the encryption module encrypts the network packets in order of priority with the highest-priority network packet being processed first.

Claim 17 (original) The network packet management system of claim 16, wherein the encryption module receives a higher-priority network packet during the encryption of the highest-priority network packet and suspends encryption of the highest-priority network packet and encrypts the received higher-priority network packet.

Claim 18 (original) The network packet management system of claim 15, wherein the decryption module decrypts the network packets in order of priority with the highest-priority network packet being processed first.

Claim 19 (original) The network packet management system of claim 18, wherein the decryption module receives a higher-priority network packet during the decryption of the highest-priority network packet and suspends decryption of the highest-priority network packet and decrypts the received higher-priority network packet.